Amendment to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claim 1 (currently amended): A method for authenticating a sender of a digital object, comprising:

recognizing a peer-to-peer (P2P) communication between a first client and a second client, said first client attempting to exchange information securely with said second client via the P2P communication without a third party mediation, said third party mediation including certificate authorities;

establishing an electronic mail protocol between the first client and the second client, said e-mail protocol, being separate from the P2P communication, comprising Simple Mail Transport Protocol (SMTP);

generating a first unique identifier (UID);

transmitting from a the first client to a previously known address of a the second client, via an the established electronic mail protocol, a first electronic mail (e-mail) message comprising the first UID, wherein the electronic mail protocol comprises a mail server operating the Simple Mail Transport Protocol (SMTP), wherein at least a portion of the electronic mail protocol operates securely using the Transport Layer Security (TLS) protocol;

receiving from the second client, via the electronic mail protocol, a second e-mail message directed to the first client comprising a second UID and a copy of the first UID;

verifying the copy of the first UID is identical to the first UID at the first client; and

transmitting from the first client to the previously known address of the second client, via the electronic mail protocol, a third e-mail message to the second client comprising a copy of the second UID;

wherein at least one of the e-mail messages transmitted to the previously known address between the first client and the second client further comprises the digital object, said digital object being used for authenticating the information to be exchanged between the first client and the second client via the P2P communication and not for authenticating the first e-mail message, the second e-mail message, or the third e-mail message.

Claim 2 (original): The method of claim 1 wherein the first message further comprises the digital object.

Claim 3 (original): The method of claim 1 wherein the third message further comprises the digital object.

Claim 4 (original): The method of claim 1 wherein the digital object is a public key for a cryptographic system.

Claim 5 (currently amended): The method of claim 4 wherein the second message further comprises a second public key for ~~a~~ the cryptographic system.

Claims 6-7 (canceled).

Claim 8 (original): The method of claim 1 wherein the first UID contains at least 128 bits.

Claim 9 (currently amended): A method for authenticating ~~the~~ a sender of a digital object, comprising:

     recognizing a peer-to-peer (P2P) communication between a first client and a second client, said first client attempting to exchange information securely with said second client via the P2P communication without a third party mediation, said third party mediation including certificate authorities;

     establishing an electronic mail protocol between the first client and the second client, said e-mail protocol, being separate from the P2P communication, comprising Simple Mail Transport Protocol (SMTP);

     receiving from ~~a~~ the first client, via ~~an~~ the established electronic mail protocol, a first electronic mail (e-mail) message comprising a first unique identifier (UID), ~~wherein the electronic mail protocol comprises a mail server operating the Simple Mail Transport Protocol (SMTP), wherein at least a portion of the electronic mail protocol operates securely using the Transport Layer Security (TLS) protocol~~;

     generating a second UID at ~~a~~ the second client;

transmitting from the second client to a previously known address of the first client, via the electronic mail protocol, a second e-mail message comprising the second UID and a copy of the first UID;

receiving conformation from the first client for verifying the copy of the first UID is identical to the first UID at the first client; and

receiving ~~from~~ at the second client, via the electronic mail protocol, a third e-mail message comprising a copy of the second UID;

wherein at least one of the e-mail messages received further comprises the digital object, said digital object being used for authenticating the information to be exchanged between the first client and the second client via the P2P communication and not for authenticating the first e-mail message, the second e-mail message, or the third e-mail message.

Claim 10 (original): The method of claim 9 wherein the first message further comprises the digital object.

Claim 11 (original): The method of claim 9 wherein the third message further comprises the digital object.

Claim 12 (original): The method of claim 9 wherein the digital object is a public key for a cryptographic system.

Claim 13 (currently amended): The method of claim 12 wherein the second electronic mail message further comprises a second public key for ~~a~~ the cryptographic system.

Claims 14-15 (canceled).

Claim 16 (original): The method of claim 9 wherein the first UID contains at least 128 bits.

Claim 17 (currently amended): A computer-readable medium including computer-executable instructions facilitating authenticating a sender of a digital object, computer-executable instructions executing the steps of:

recognizing a peer-to-peer (P2P) communication between a first client and a second client, said first client attempting to exchange information securely with said second client via the P2P communication without a third party mediation, said third party mediation including certificate authorities;

establishing an electronic mail protocol between the first client and the second client, said e-mail protocol, being separate from the P2P communication, comprising Simple Mail Transport Protocol (SMTP);

generating a first unique identifier (UID);

transmitting from ~~a~~ the first client to a previously known address of ~~a~~ the second client, via ~~an~~ the established electronic mail protocol, a first electronic mail (e-mail) message comprising the first UID~~, wherein the electronic mail protocol comprises a mail server operating the Simple Mail Transport Protocol (SMTP), wherein at least a portion of the electronic mail protocol operates securely using the Transport Layer Security (TLS) protocol~~;

receiving from the second client, via the electronic mail protocol, a second e-mail message directed to the first client comprising a second UID and a copy of the first UID;

verifying the copy of the first UID is identical to the first UID at the first client; and

transmitting from the first client to the previously known address, via the electronic mail protocol, a third e-mail message to the second client comprising a copy of the second UID;

wherein at least one of the messages transmitted to the previously known address further comprises the digital object, said digital object being used for authenticating the information to be exchanged between the first client and the second client via the P2P communication and not for authenticating the first e-mail message, the second e-mail message, or the third e-mail message.

Claim 18 (original): The computer-readable medium of claim 17 wherein the digital object is a public key for a cryptographic system.

Claim 19 (currently amended): The computer-readable medium of claim 18 wherein the second message further comprises a second public key for ~~a~~ the cryptographic system.

Claim 20 (currently amended): An apparatus for authenticating ~~the~~ a sender of a digital object, comprising:

      a random number generator generating a first unique identifier (UID);

      a network interface <u>recognizes a peer-to-peer (P2P) communication between a first client and a second client, said first client attempting to exchange information securely with said second client via the P2P communication without a third party mediation, said third party mediation including certificate authorities;</u>

      <u>wherein the network interface establishes an electronic mail protocol between the first client and the second client, said e-mail protocol, being separate from the P2P communication, comprising Simple Mail Transport Protocol (SMTP);</u>

      <u>wherein the network interface transmits</u> ~~transmitting~~ to a previously known address, via ~~an~~ <u>the established</u> electronic mail (e-mail) protocol, a first e-mail message comprising the first UID~~, wherein at least a portion of the electronic mail protocol operates securely using the Transport Layer Security (TLS) protocol~~;

      <u>wherein</u> the network interface <u>receives</u> ~~receiving~~, via the electronic mail protocol, a second e-mail message comprising a second UID and a copy of the first UID, wherein the copy of the first UID and the first UID is compared for verification; and

      <u>wherein</u> the network interface <u>transmits</u> ~~transmitting~~ to the previously known address, via the electronic mail protocol, a third e-mail message comprising a copy of the second UID;

      wherein at least one of the messages transmitted to the previously known address further comprises the digital object<u>, said digital object comprises a public key used for authenticating the information to be exchanged between the first client and the second client via the P2P communication and not for authenticating the first e-mail message, the second e-mail message, or the third e-mail message</u>.